兵庫県情報セキュリティ監査業務委託仕様書

令和６年８月

兵庫県企画部デジタル改革課

1　調達件名

兵庫県情報セキュリティ監査業務委託

2　概要

本調達では、次の２つの業務を委託する。

(1) 情報システム外部監査

兵庫県（以下「県」という。）では情報システムのセキュリティ確保のため、外部からのサイバー攻撃に備えるための技術的セキュリティ監査を外部事業者に委託し、その他の監査項目については県内部で対応してきた。

これに加えて、令和４年度から、運用管理体制や個人情報の管理方法のチェック等、物理的・人的セキュリティ等に着目した外部監査を実施している。

指定する県情報システムのセキュリティが適正に確保されているか否かを点検・評価し、問題点の確認、改善方法等についての検討・助言・指導を行う。

業務詳細は、別紙１で定める。

(2) β´モデル採用自治体における外部監査

県行政情報ネットワーク（以下「県庁 WAN」という。）は、総務省の「地方公共団体における情報セキュリティポリシーに関するガイドライン（以下「ポリシーガイドライン」）という。」に基づき、インターネット接続系、LGWAN 接続系及び個人番号利用事務系に分離する「三層の対策」を実施している。令和３年度からは、インターネット接続系に重要な情報資産を設置するβ´モデルを採用し運用している。

ポリシーガイドラインにおいて、β´モデルを採用する場合は３年度毎の外部監査結果を地方公共団体情報システム機構に提出することが定められているが、令和３年度の初回監査から既定の年数が経過した。

総務省指定の監査項目に基づき、ネットワーク分離が適切に実施されているかを点検・評価し、問題点の確認、改善方法等について検討・助言・指導を行う。

業務詳細は、別紙２で定める。

3　契約期間

契約日から令和７年３月 31 日まで

4　想定スケジュール

想定スケジュールは図１のとおりとする。ただし、実施詳細は、県と調整の上、進めること。

項目	8 月	9 月	10 月	11 月	12 月	1 月	2 月
入札～契約							
計画書の策定							
組織・人・技術的調査							
報告会・改善指導							
報告書確認・修正							

図１.想定スケジュール

5　受託者の要件

(1) 監査チームの資格要件

監査責任者、監査人、監査補助者、技術責任者等で構成される監査チームを編成し、同チームには、情報セキュリティ監査に必要な知識及び経験（地方公共団体における情報セキュリティ監査の実績）を持ち、次に掲げるいずれかの資格を有する者が１人以上含まれていること。

①　システム監査技術者
②　公認情報システム監査人（CISA）
③　公認システム監査人
④　ISMS 主任審査員
⑤　ISMS 審査員
⑥　公認情報セキュリティ主任監査人
⑦　公認情報セキュリティ監査人
⑧　情報処理安全確保支援士

(2) 実績要件

監査チームには、監査の効率と品質の保持のため次のいずれかの実績（実務経験）を有する専門家が、上記（１）とは別に１人以上含まれていること。

①　情報セキュリティ監査
②　情報セキュリティに関するコンサルティング
③　情報セキュリティポリシーの作成に関するコンサルティング（支援を含む）

(3) 入札参加要件

受託者（企業グループの構成員を含む）は、監査対象の県庁 WAN 上の情報システムの開発・運用等の調達、機器等の調達等（但し、企画、コンサル、調達支援のみの場合は除く）には、参加していないこと(再委託先事業者も同様とする)。

6　受託者の権限

受託者は、本件監査を実施するため県に具体的な必要性を説明して、相当な方法をもって、次に掲げる行為を行うことができる。

- 県の所有・管理する場所に存する各種の文書類及び資料類の閲覧、収集
- 県の役職員に対する質問及び意見聴取
- 県の施設の現地調査
- 監査技法を適用するためのコンピュータ機器の利用
- 本件監査の監査報告書を決定する前における県との意見交換

7　受託者の義務

受託者は、次の義務を負う。

(1) 品質管理義務

監査結果の適正性を確保するために、適正な品質管理を行うこと。

(2) 平易な説明義務

受託者は、できる限り専門用語を避け、理解しやすい平易な説明を行うこと。

(3) 注意義務

受託者は、職業倫理に従い専門職としての相当の注意を持ち、誠実に本件監査を実施し、監査従事者全員をして受託者の義務を履行させること。

8　作業時間

現地調査やヒアリング等、県の施設内で行う作業については、原則として県の勤務時間内（休日を除く日の８時 45 分～17 時 45 分）に行うものとする。

ただし、技術的検査については、サーバの利用用途、稼働時間等を考慮し、県と協議のうえ作業時間を決定すること。

その他、具体的な作業日時等については、県との協議のうえ決定すること。

9　成果物の納品方法

(1) 形式

- 電子媒体（CD-ROM または DVD-ROM）版と製本版に編纂し、納品すること。
- 部数は指定がない限り、各１部とする。
- 納入に必要な資材は、受託者において用意すること。
- 製本版は、原則として A4 判の用紙を使用し、種類別にチューブファイル等に収め、背表紙等には内容を簡記すること。ただし、必要に応じて A3 判で作成してもよい。
- 電子媒体の表面には収録内容を簡記すること。
- 電子データは、Microsoft Office 2016 以降で編集できること。

(2) 場所

第 11 項に記載の業務主管課に収めること。

10　留意事項

(1) 契約不適合責任

引き渡された目的物が種類、品質又は数量に関して契約の内容に適合しない場合、県は受託者に対し、履行の追完を請求することができる。

履行の追完は、民法第 562 条第１項本文にかかわらず、代替物の引渡し又は不足分の引渡しの方法によること。

(2) 機密保持

本業務遂行上知り得た情報を第三者に漏らしてはならない。また、本契約が終了し、又は解除された後においても同様とすること。

(3) 法令等の順守

県情報セキュリティ対策指針、個人情報保護法等を順守すること。また、法令及び契約書の別記「個人情報取扱特記事項」を遵守すること。

(4) 知的財産の取扱い

ア　成果物及びこれに付随する資料は、全て県に帰属するものとし、書面による県の承諾を受けないで他に公表、譲渡、貸与又は使用してはならない。ただし、成果物及びこれに付随する資料に関し、受託者が従前から保有する著作権は受託者に留保されるものとし、県は、

本業務の目的の範囲内で自由に利用できるものとする。

イ　本委託業務で得られた成果物の著作権（著作権法（昭和45年法律第48号）第27条、第28条の権利を含む。）を無償で県に譲渡すること。

ウ　本委託業務で得られた成果物に著作者人格権を行使しないこと。また、本委託業務で得られた成果物に第三者の著作者がある場合は、当該著作者に著作者人格権を行使しないように必要な措置をとること。

エ　本委託業務によって得られた成果物について、県が使用する権利及び県が第三者に使用を許諾する権利を無償で許諾すること。

オ　特許権、著作権等の知的財産権の対象となっている第三者の技術等を使用するときは、その使用に関する一切の責任を負う。また、それに関わる費用については受託者の負担とする。

(5) 再委託

ア　受託者は、委託業務の全部又は主体的部分（委託業務における総合的な企画及び判断並びに業務遂行管理部分）を一括して第三者に委任し、又は請け負わせてはならない。

イ　受託者は委託業務の一部を第三者に委任し、又は請け負わせ（以下「再委託等」という。）てはならない。ただし、あらかじめ再委託等の相手方の住所、氏名及び再委託等を行う業務の範囲等を記載した、再委託の必要性がわかる書面を県に提出し、県の書面による承認を得た場合は、受託者は、県が承認した範囲の業務を第三者に再委託等することができるものとする。

(6) 疑義の解釈

本仕様書に定めのない事項及び疑義の生じた場合には、県と受託者の協議により定めるものとする。

11　業務主管課

県企画部デジタル改革課
〒650-8567　兵庫県神戸市中央区下山手通5-10-1（県庁第3号館12階）
TEL　078-362-3051　FAX 078-362-3931　Mail　sysad@pref.hyogo.lg.jp

別紙１

情報システム外部監査

詳細仕様

1　監査対象

別添１「監査対象システム一覧」に掲げる 30 システム

ただし、契約締結後、セキュリティインシデントの発生等、監査対象を別システムに変更すべき事由が生じた場合は、県と受託者双方協議のうえ、監査対象を変更することがある。

2　監査概要

県情報システムのセキュリティが適正に確保されているか否かを物理的・人的・技術的セキュリティを中心に点検・評価し、問題点の確認、改善方法等についての検討・助言・指導を行うことを目的とする。

3　履行場所

県庁第３号館 12・13 階（兵庫県企画部デジタル改革課)、
監査対象システム設置場所他

4　監査基準

(1) 必須とする基準

ア　県情報セキュリティ対策指針（以下「県指針」という。）

イ　県行政情報ネットワーク運用管理要綱

(2) 参考とする基準

ア　地方公共団体における情報セキュリティポリシーに関するガイドライン

イ　地方公共団体における情報セキュリティ監査に関するガイドライン

ウ　各監査対象システムの運用管理要綱

エ　その他情報セキュリティに関し有用な基準等は、県と協議のうえ採用すること。

5　監査計画の策定

受託者は、契約締結後２週間以内に、県に次の事項を含む監査手順及びその実施時期を記載した「監査実施計画書」を提出し、承認を得ること。

・監査対象及び範囲
・実施方法
・実施スケジュール
・監査の実施体制
・進捗管理及び報告方法

・監査結果の報告の日時・内容
・その他、監査実施時に必要な事項

6　書面監査の実施

(1) 調査票（チェックシート）の作成

ア　書面監査のため、監査対象システムの県指針第 10 条に規定する運用管理者（以下「運用管理者」という。）に配布し、情報システムの状況を照会する、調査票（チェックシート）を作成すること。なお、調査票の監査項目は、前年度監査結果との比較を想定し、原則として令和５年度調査票改訂版（別添２）と同じ項目を含むこととし、監査対象システムの性質上、固有の項目が追加となる場合は別紙として作成すること。

イ　調査票は、県指針等への対応を中心に項目を設定すること。ただし、単に県指針等の各項目を列挙するのではなく、同指針等で求められている内容を、必ずしも情報システムに習熟しているとは限らない運用管理者の担当職員にも分かりやすい表現に落とし込みながら、監査に必要な情報を得られる内容とすること。

ウ　調査票の内容については、配布前に県に提出し、承認を得ること。

エ　運用管理者への調査票の配布は県が行うが、運用管理者からの質問受付とその回答、調査票の回収、追加資料の依頼等は、原則として受託者が運用管理者と直接行うこととし、県に適宜状況を共有すること。ただし、運用管理者との応対で疑問等が生じた場合は、運用管理者への連絡前に県に相談することとする。

オ　書面監査にあたり、監査対象システムの運用管理要綱、仕様書や完成図書等の資料収集が必要な場合は、調査票に必要となる資料を明記し、運用管理者に提出を求めること。

(2) 調査票の分析・評価

運用管理者、担当者及び職員等へのインタビューにより調査し、必要に応じて、職員等へのアンケート調査を実施して確認すること、調査票の回答内容を基に監査を行うこと。

7　実地監査の実施

(1) 書面監査の結果、または県と受託者との協議の結果、より詳細な監査の必要性が認められたシステムについて、運用管理者へのヒアリング、当該システムの運用管理に係る各種帳簿等の追加チェックや現地調査（必要な場合）等を行う、実地監査を実施すること。

(2) 実地監査の対象システム数は 10 を上限とする。
(3) 運用管理者との調整（日程や場所等）は県が中心となって実施するが、受託者もこれに協力すること。また、ヒアリング項目の作成や監査対象となる帳票等の指定については受託者で対応すること。
(4) 実地監査に際し、直接システムの設置場所を確認する必要がある場合は、これに対応すること。なお、運用管理者へのヒアリングについては原則対面での実施とするが、やむを得ない理由がある場合は Web 会議等による実施も可とする。

8　技術監査の実施

(1) 下記の脆弱性検査ツール（ネットワークスキャナ）から最低１つ以上選択して使用し、ハードウェア・ソフトウェア・Web アプリケーション等の脆弱性、修正プログラムの適用の有無等を確認するとともに、発見された脆弱性について具体的な解決方法を提示すること。

・Nessus
・ZAP
・Nikto
・Penetrator Vulnerability Scanner
・QualysGuard
・Rapid7 nexpose

(2) 技術監査の対象となるサーバは、監査対象システムのサーバのうち代表的なものとする。

なお、インターネット上に公開されているサーバは、県において別途監査を実施するため対象外とする。ただし、県立病院の電子カルテシステム等の非公開外部接続機器は対象とする場合がある。

(3) 技術監査の際には、以下の点に留意すること。

ア　使用するツールは事前に書面で県に報告し、承諾を得ること。
イ　ファイアウォールやフィルタリングシステムで隔てられた場所からではなく、県の指定する、対象サーバと同セグメントから監査を実施すること。
ウ　対象サーバに障害を生じさせないよう、細心の注意をもって業務を行うこと。もし障害が発生した場合は、県に速やかに報告するとともに、障害の解消のため、県及び県庁 WAN や各情報システムの維持管理業者に協力して対応にあたること。
エ　技術監査の実施中に、情報漏えい等につながる危険性が高い脆弱性等が検出された場合には、その内容及び改善策について速やかに

県に報告すること。

オ　技術監査においては、使用したツールのログや通信のログを取得するなど検査の内容を確実に記録し、県にログを提供すること。

カ　県が必要と判断した場合、対象機器のログを確認すること。

キ　県が必要と判断した場合、サーバ等の設定ファイル等を確認し、問題点を指摘するとともに改善策について助言を行うこと。

9　フォローアップ

昨年度実施した情報セキュリティ監査の監査報告書で指摘された改善事項について、被監査部門の対応状況を確かめるため、フォローアップを実施すること。対象件数は 29 システムとすると。

10　監査報告書の作成

(1) 改善策の明記

調査報告書には、各監査により検出された問題点や脆弱性等を指摘事項として示すとともに、指摘事項に対し、具体的な改善策を記載すること。

(2) 監査報告書の作成様式

ア　Ａ４版縦（必要に応じてＡ３版三つ折も可。Ａ３版三つ折の場合、両面印刷は 不可とする。）とする。

イ　様式は任意とするが前年度の報告様式に準じて作成すること。

ウ　監査報告書は、次の３種類を作成し、提出すること。

①　監査対象についての脆弱点を網羅した「情報セキュリティ監査報告書(全体版)」(非公開)

②　全ての監査対象システム毎にレポートを作成した「情報セキュリティ監査報告書(各システム版)」(非公開)

③　全庁公開にそぐわない内容 (セキュリティホールの詳細情報等) を省略した、公開を前提とする「情報セキュリティ監査報告書(公開版)」

(3) 監査報告書の宛先

(2) ウ①及び③の報告書は県指針第８条に規定する情報セキュリティ対策統括者（以下「統括者」という。）宛て、(2) ウ②の報告書は運用管理者宛てとすること。

11　監査報告会

統括者及び監査対象となった情報システムの運用管理者に対して、監査結果の報告会を実施すること。

(1) 統括者への報告

書面監査、実地監査及び技術監査の結果について、10(2)ウ①～③の監査報告書により、統括者に対面で説明すること。ただし、やむを得ない理由がある場合はWeb会議等による実施も可とする。

(2) 運用管理者への報告

ア　全ての監査対象システム毎に 10(2)ウ②の監査報告書により書面で報告すること。

イ　指摘事項が多数確認されたシステム等について、アにかかわらず、12に掲げる改善指導の内容を運用管理者に対面で説明すること。ただし、やむを得ない理由がある場合はWeb会議等による実施も可とする。

ウ　イの対象システムは、県と受託者で協議の上決定する。

エ　運用管理者との調整（日程や場所等）は受託者が中心となって実施すること。

12 改善指導

監査結果に基づき次の改善指導を実施すること。

(1) 運用管理要綱等の作成・修正の指導

監査の結果、監査対象システムの運用管理要綱等に作成・修正の必要がある場合は、その内容を具体的に示すことと。

(2) 物理的、人的な脆弱性改善の指導

監査の結果、監査対象システムの物理的・人的な脆弱性が判明し、改善する必要がある場合は、改善案を具体的に示すこと。

(3) システム上の脆弱性改善の指導

監査の結果、監査対象システム上の脆弱性が判明し、改善する必要がある場合は、改善案を具体的に示すこと。

(4) 関係者への改善の指導

監査の結果、必要と認められる場合は、改善案を開発・運用等の受託業者やその他関係者に対して、改善の手順・方法等を具体的に説明し、改善を指導すること。

なお、当該脆弱性検出及び改善部分については、助言型監査とすること。

13 監査成果物

次に掲げる監査成果物を提出すること。

(1) 監査実施計画書

(2) 情報セキュリティ監査報告書（全体版）

(3) 情報セキュリティ監査報告書（各システム版）

(4) 情報セキュリティ監査報告書（公開版）

(5) 監査の過程で収集した各種ログ（電子媒体のみ納品）

別紙２

β´モデル採用自治体における外部監査
詳細仕様

1　監査対象

県庁 WAN

2　監査概要

インターネット接続系、LGWAN 接続系及び個人番号利用事務系が適正な情報セキュリティレベルで分離し、安全に稼働しているかを監査する。

3　履行場所

県庁３号館 12 階・13 階（兵庫県企画部デジタル改革課）他

4　監査項目

ポリシーガイドラインと併せて総務省が策定した「地方公共団体における情報セキュリティ監査に関するガイドライン」（以下「監査ガイドライン」という。）の第３章「情報セキュリティ監査項目」のうち、次の項目とする。（別添３参照）

(1) βモデル・β’モデル共通の監査項目

β/β’モデルの採用にあたり必須となる、監査に関するガイドラインにおける組織的・人的対策に係る監査項目（23 項目）

(2) β’モデル固有の監査項目

β’モデルの場合：同「3.12. β’モデルを採用する場合の追加監査項目」（13 項目）

5　監査基準

(1) 必須とする基準

ア　地方公共団体における情報セキュリティポリシーに関するガイドライン

イ　地方公共団体における情報セキュリティ監査に関するガイドライン

ウ　県情報セキュリティ対策指針（県の情報セキュリティポリシー、以下「県指針」という。）

エ　兵庫県行政情報ネットワーク運用管理要綱

オ　マイナンバー利用事務用ネットワーク運用管理要綱

(2) 参考とする基準

ア　個人情報保護法

イ　県情報セキュリティ監査部会設置要領

ウ　その他情報セキュリティに関し有用な基準等で、県と協議して採用するもの

6　監査計画の策定

受託者は、契約締結後２週間以内に、県に次の事項を含む監査の手順及びその実施時期を具体的に記載した「監査実施計画書」を提出し、承認を得ること。

・監査の対象及び範囲
・実施方法
・実施スケジュール
・委託先の実施体制
・進捗管理及び報告方法
・監査結果の報告の日時・内容
・その他、監査実施時に必要な事項

7　組織・人的調査の実施

(1) 基準等の検査

監査資料のレビュー並びに県指針第８条に規定する情報セキュリティ対策統括者（以下「統括者」という。）、県指針第 10 条に規定する運用管理者（以下「運用管理者」という。）等へのインタビューにより、必要な基準、規定等が策定されているかを確認すること。

(2) 職員への聞き取り調査

運用管理者、担当者及び職員等へのインタビュー、執務室の視察により調査し、必要に応じて、職員等へのアンケート調査を実施して確認すること。

(3) 職員アンケートの実施

県職員（約 12,000 人）を対象としたアンケートを実施し、その結果をＣＳＶデータ等で提出すること。受託者は、受領した電子データを集計し、職員の指針の理解度や意識、所属組織、職位等による傾向を分析し、評価すること。

8　監査報告書の作成

(1) 改善策の明記

調査報告書には、各監査により検出された問題点や脆弱性等を指摘事項

として示すとともに、指摘事項に対し、具体的な改善策を記載すること。

(2) 監査報告書の作成様式

ア　Ａ４版縦（必要に応じてＡ３版三つ折も可。Ａ３版三つ折の場合、両面印刷は 不可とする。）とする。

イ　様式は任意とするが、県が別途作成する総務省報告様式への転記が容易になるよう、4 項の監査項目に対する指摘事項・改善方針を表形式でまとめた内容を含むこと。

ウ　監査報告書は監査対象についての脆弱点を網羅した非公開の「情報セキュリティ監査報告書(詳細版)」と公開を前提とした「情報セキュリティ監査報告書(公開版)」の２種類を作成し、提出すること。

(3) 監査報告書の宛先

統括者宛てとすること。

9　監査報告会

統括者及び監査対象となった情報システムの運用管理者に対して、監査結果の報告会を実施すること。

10　改善指導

監査結果に基づき次の改善指導を実施すること。

(1) 指針等の作成・修正

監査の結果、指針、基準、要綱等の作成・修正の必要がある場合は、案作成について具体的に指導すること。

(2) 組織的、人的な脆弱性改善の指導

監査の結果、組織的、人的な脆弱性が判明し、改善する必要がある場合は、改善案作成について具体的に指導するとともに、必要に応じて職員研修を実施すること。

(3) 関係者への改善の指導

監査の結果、必要と認められる場合は、改善案を開発・運用等の受託業者やその他関係者に対して、改善の手順・方法等を具体的に説明し、改善を指導すること。

なお、当該脆弱性検出及び改善部分については、結果を保証する保証型監

査とすること。

11　監査成果物

次に掲げる監査成果物を提出すること。

(1) 監査実施計画書

(2) 情報セキュリティ監査報告書（詳細版）

(3) 情報セキュリティ監査報告書（公開版）

（別添１）令和６年度　監査対象システム一覧

No	システム名	部	課室
1	図書検索システム	県議会	調査課：図書室
2	クラウドメール（議員）	県議会	総務課
3	兵庫県ホームページ	総務部	広報広聴課
4	適用業務システム 恩給	総務部	職員課
5	学内情報基盤システム(事務系ネットワークシステム)	総務部	教育課（兵庫県立大学）
6	総合財務会計システム 公有財産管理	総務部	管財課
7	人事給与システム	企画部	デジタル改革課
8	ひょうご子育て応援の店携帯認証システム	県民生活部	男女青少年課
9	「ひょうご防災ネット」アプリクラウド化事業	危機管理部	災害対策課
10	情報事務センター情報システム	福祉部	福祉部　総務課
11	指定難病等医療費助成システム	保健医療部	疾病対策課
12	肝炎医療費助成システム	保健医療部	疾病対策課
13	治山業務支援システム	農林水産部	治山課
14	適用業務システム漁業近代化資金利子補給	農林水産部	水産漁港課
15	農業用防災ダムシステム	農林水産部	農地整備課
16	浄化槽台帳システム	環境部	環境整備課
17	適用業務システム 道路現況	土木部	道路保全課
18	流域下水道事業資産台帳システム	土木部	下水道課
19	電子納品保管管理システム	土木部	契約管理課
20	土砂災害情報提供システム	土木部	砂防課
21	河川情報総合管理システム（警報システム）	土木部	河川整備課
22	水道・工水事業管路情報システム	企業庁	水道課
23	淡路医療センター電子カルテシステム	病院局	県立淡路医療センター
24	丹波医療センター電子カルテシステム	病院局	県立丹波医療センター
25	ひょうごこころの医療センター電子カルテシステム	病院局	県立ひょうごこころの医療センター
26	医局インターネット（メール）	病院局	病院局：経営課
27	千種川流域 河川情報システム 水守	西播磨県民局	光都土木事務所
28	兵庫県公立学校教員採用試験システム	教育委員会事務局	教職員人事課
29	県立図書館インターネット予約貸出システム	教育委員会事務局	社会教育課
30	特別支援教育就学奨励費システム	教育委員会事務局	財務課

＜備考＞

監査対象を別システムに変更すべき事由が生じた場合は、県と受託者双方協議のうえ、監査対象を変更することがある。

（別添２） 令和５年度調査票　改訂版　記載例

システム名	○○システム
課室名	○×課
担当者名	○○　××
内線	内線○○○○

No	大区分	中区分	小区分	設問	回答	備考欄	提出物
1	情報資産の分類		情報資産の分類	情報資産をその内容に応じて分類し、その重要度に応じて分類していますか？	2.概ねしている		・情報資産管理台帳
2			実施手順	情報システムの適正な運用を図るために必要な情報セキュリティ対策の実施手順（システム運用管理要綱）を策定していますか？	1.している		・システム運用管理要綱
3			要綱	指針及び運営管理要綱の遵守状況を定期的に点検し、支障を認めた場合には迅速かつ適切な措置を講じていますか？	1.している		
4	物理的セキュリティ対策	機器の設置	火災・水害、ほこり、振動等の排除	通信機器やサーバ等は、火災、水害、温度等の影響を可能な限り排除した場所に設置し、固定用ベルト、アンカーで固定する等の措置を講じていますか？	1.している		
5			耐震、免震化	重要な通信機器やサーバ等を設置する場合に、機器の固定等の耐震対策だけでなく、免震ラックに設置する等の措置を講じていますか？	1.している		
6			配線の保護	機器等の配線が損傷を受けないよう、カバー・収納管に収納するなどしていますか？	1.している		
7			接続口の隔離	ネットワークのスイッチやハブのネットワーク接続口は、第三者が容易に接続できないように、隠ぺい、閉鎖等の措置がされていますか？	2.概ねしている		
8		設置場所	設置場所	システム機器の設置場所はどこですか？【複数選択可】 1.[redacted]号館[redacted]階、2.[redacted]号館[redacted]階、3.[redacted]棟、4.庁内別サーバ室、5.執務室内、6.[redacted]データセンター、7.[redacted]データセンター、8.[redacted]データセンター、9.クラウド利用（AWS,Google,Azure等）、10.LGWAN-ASP、 11.その他（具体的に）	☑ 1.　号館　階 ☐ 2.　号館　階 ☐ 3. ☐ 4. 庁内別サーバ室 ☐ 5. 執務室内 ☑ 6.　　データセンター ☐ 7.　　データセンター ☐ 8.　　データセンター ☐ 9. クラウド利用(AWS,Google,Azure等) ☐ 10. LGWAN-ASP ☐ 11. その他（具体的に備考欄へ記入）		
9			耐震、防火、防犯対策	情報システム室には、耐震対策、防火対策、防犯対策等の措置を講じていますか？	1.している		
10			入退室の管理	情報システム室の入退出はあらかじめ許可した者のみとし、入退室管理簿の記載等を行っていますか？	1.している		・入退室管理簿
11			入退室管理、名札・身分証明書の携帯	情報システム室に入室する者は、身分証明書等を携帯し、運用管理者の指定する担当職員の求めに従い提示していますか？	1.している		
12	人的セキュリティ対策	情報資産の管理	データのバックアップの作成	重要な情報資産について、データのき損、滅失等に備えるため、保管するデータのバックアップを定期的に作成していますか？	2.概ねしている		・バックアップ管理表(記録簿)
13			データの暗号化	機密性の高い情報を外部へ送信、提供する場合、必要に応じ暗号化又はパスワード設定を行っていますか？	2.概ねしている		
14		記録媒体の管理等	データの媒体又は電子メール等による持出し	個人情報、機密情報等が記録されたUSBメモリ、DVD、ハードディスク等の電子媒体を持ち出す場合は、データの暗号化、パスワードによる保護を行っていますか？	1.している		
15			記録媒体の廃棄	USBメモリ、DVD、ハードディスク等の電子媒体が不要となった場合は、データを復元できないように消去を行ったうえで廃棄していますか？	1.している		・記録媒体の廃棄記録
16		IDパスワード及びの管理	パスワード安全性１	パスワードの桁数は最低何桁以上ですか？	4. 7桁		
17			パスワード安全性２	パスワードは英数記号等を混在させていますか？	1.している		
18		教育・訓練	情報セキュリティ対策に関する研修・普及啓発	システム利用者に情報セキュリティ研修、標的型攻撃訓練等を年1回以上受講させていますか？	3.どちらとも言えない		・情報セキュリティ研修、標的型攻撃訓練記録簿
19			不測事態に備えた訓練の計画的な実施	情報システム管理者、情報システム担当者がセキュリティインシデントが発生した場合の訓練を年1回以上受講していますか？	3.どちらとも言えない		・セキュリティインシデント訓練の記録
20		事故等の報告	過去の報告	過去に情報の漏えいやシステムに重大な障害が生じた場合、速やかに統括者に報告しましたか？ ※障害等が発生したことがない場合、1を選択して備考にその旨記載	1.している	過去に重大な障害なし	
21			報告手順の確認	情報の漏えいやシステムに重大な障害が生じた場合の報告先と報告手順を知っていますか？	2.概ね把握している		・障害発生報告手順
22			契約	システムの開発・運用等を事業者等に委託しようとする場合は、関連法令、県情報セキュリティ対策指針、その他遵守すべき事項を明記した契約を締結していますか？	1.している		・委託契約書（仕様書、個人情報取扱特記事項を含む） ・賃貸借契約書（委託部分を含む場合）

No	大区分	中区分	小区分	設問	回答	備考欄	提出物
23		外部委託に関する管理	個人情報取扱特記事項	個人情報を取り扱う事務を委託する場合は、契約書に個人情報取扱特記事項（「個人情報を取り扱う事務の委託に伴う措置について（平成9年11月2日1付け文第294号知事公室長通知）」）を規定していますか？	1.している		
24			損害賠償	委託事業者との契約書には、この契約仕様、要綱等が遵守されなかったことにより損害が発生した場合の賠償等の規定を定めていますか？	1.している		
25			再委託の承認	再委託、再々委託等を行う場合には、相手方の氏名、業務の範囲、その必要性、体制等を記載した書面の提出を受け、再委託事業者等の安全管理措置を確認のうえ書面で承認していますか？	1.している		・再委託申請書 ・再委託承認書
26			データ受け渡し	委託事業者とのデータの受け渡しに係る内容、日付等を記録していますか？	2.概ねしている		・委託事業者とのデータ受け渡し記録簿
27			名簿作成	委託事業者の責任者や業務に従事する者の氏名、作業場所等を記載した名簿を作成していますか？	2.概ねしている		
28			身分証明の確認	委託事業者に身分証明書を携帯させ、必要に応じて提示を求めていますか？	1.している		
29			従事者に対する教育	委託事業者の従業員に対する教育が実施されているかを確認していますか？	2.概ねしている		・委託事業者への確認記録
30	技術的セキュリティ対策	アクセス記録の取得等	各種アクセス記録の保存	各種アクセス記録等情報セキュリティ対策に必要な記録を取得し、1年間以上（個人番号利用事務は７年以上）、保存していますか？	3.どちらとも言えない		
31			アクセス記録等の分析、監視	定期的にアクセス記録等を分析、監視していますか？	2.概ねしている		・アクセス記録の分析記録
32		情報システムにおけるアクセス制御	利用者管理	利用者IDの登録、変更、退職した利用者の抹消等の取扱いに関わる手続を定め、利用者を適正に管理していますか？	2.概ねしている		
33			アクセス制御	情報通信機器にセキュリティ上の問題が認められ、情報資産に脅威が生じるおそれがある場合には、速やかに当該情報通信機器を内部ネットワークから遮断できますか？	1.している		
34		外部ネットワークとの接続	外部ネットワークの有無	県以外の機関が管理する情報システム（以下「外部ネットワーク」という。）との接続口を持っていますか？ ※「持っていない」と回答した場合、No.38へ。（No.35～37は回答不要）	1.持っている		
35			外部ネットワークの回線種別	外部との物理的接続回線は何ですか？【複数選択可】 専用線、IP-VPN、広域イーサネット、インターネットVPN、エントリーVPN、その他（具体的に）	☐ 1.専用線 ☑ 2.IP-VPN ☐ 3.広域イーサネット ☐ 4.インターネットVPN ☐ 5.エントリーVPN ☐ 6.その他（備考欄に具体的に記載）		
36			ファイアウォールの設置	外部ネットワークと接続する場合、ファイアウォールの設置、論理的なネットワークの分割等、適切なネットワーク経路制御を講じている。	1.している		
37			ユーザ認証、ファイアウォールの設置	外部からの接続時の認証方法をお答えください。 パスワードのみ、ユーザ名・パスワード、多要素認証、その他(具体的に)	3.多要素認証		
38		コンピュータウイルス対策	ウイルスチェック	外部のネットワークからデータを取り入れる際には、利用者端末等においてウイルスチェックを行い、システムへの侵入を防止していますか？	2.概ねしている		
39			コンピュータウイルス情報	EMOTET、ランサムウェア等のコンピュータウイルスが流行した場合、その情報について利用者に対する注意喚起を行っていますか？	2.概ねしている		
40			ウイルスチェック用のパターンファイル更新	システムで独自に利用するパソコンやサーバのウイルスチェック用のパターンファイルは常に最新のものに更新していますか？	1.している		
41			コンピュータウイルスに対する修正プログラムの入手	コンピュータウイルス等のセキュリティ修正プログラムの入手に努め、端末、情報通信機器、サーバ等に速やかに適用していますか？	1.している		
42		不正アクセス対策	ポート管理（ネットワーク上のサーバがサービスを区別	通信機器、サーバ等のftp、telnet、smtp等の不要なポートは、ファイアウォールや機器設定で閉じていますか？	1.している		
43			不要なユーザＩＤの削除	不正アクセスを防止するため、端末、サーバ、通信機器及び端末上の不要な利用者IDは速やかに削除していますか？	3.どちらとも言えない		不要なユーザＩＤの削除記録
44			セキュリティホール対策	不正アクセスを防止するため、サーバや通信機器のセキュリティホールに対しては、速やかに修正プログラムを適用していますか？	1.している		
45			Webサーバ保護	Webサーバについては、WAF、Webページ改ざんの検出する措置等を実施していますか？	4.あまりしていない		
46			不正アクセス	不正アクセスを受けるおそれが認められる場合には、勤務時間外でもシステムの停止を含む必要な措置は可能にしていますか？	2.概ねしている		

No	大区分	中区分	小区分	設問	回答	備考欄	提出物
47	運用面の対策	外部（クラウド）サービス利用の対策	外部（クラウド）サービス利用の有無	外部（クラウド）サービス（インターネット、専用回線等により接続された情報システムが提供するサービス）を利用していますか？ ※　利用していない」と回答した場合、No.55へ。（No.48～54は回答不要）	2.していない		
48			外部（クラウド）利用形態	外部（クラウド）サービスの利用形態をお答えください【複数選択可】 1. ホームページのホスティング、2. ファイル保管・データ共有、3. サーバ利用、4. データバックアップ、5. 情報共有・ポータル、6. スケジュール共有、7. LGWAN-ASP、 8. その他（具体的に）	☐ 1. ホームページのホスティング ☐ 2. ファイル保管・データ共有 ☑ 3. サーバ利用 ☐ 4. データバックアップ ☐ 5. 情報共有・ポータル ☐ 6. スケジュール共有 ☐ 7. LGWAN-ASP ☐ 8. その他（備考欄に具体的に記載）		
49			外部（クラウド）利用のセキュリティ	外部（クラウド）サービスを利用するに当たり、データセンター、通信回線等の情報の流通経路全般にわたるセキュリティ対策の状況を確認していますか？	1.している		
50			外部（クラウド）のバックアップ	外部（クラウド）環境のデータについて、バックアップを取得していますか。	1.している		バックアップの記録
51			外部（クラウド）の停止	外部（クラウド）サービスが中断・停止した場合の対策を検討し、委託先を選定する際の要件としていますか？	1.している		
52			外部サービスの選定	外部サービスを利用しようとする場合は、利用目的及び業務範囲を明確にするとともに、取り扱う情報の内容に応じ、情報の保存場所、裁判管轄、準拠法等のリスクの対策を検討した上で、外部サービスの提供者を選定していますか？	2.していない		外部サービス選定基準
53			外部サービスの許可	外部サービスにおいて非公開情報を取り扱う場合は、あらかじめ統括者の許可を得ていますか？また、外部サービスの提供者が不特定多数の利用者に対して提供する画　的な約款、規約等への同意のみで利用が可能となる外部サービスでは、原則として非公開情報を取り扱ってはいませんか？	☐ 1. ホームページのホスティング ☐ 2. ファイル保管・データ共有 ☐ 3. サーバ利用 ☐ 4. データバックアップ ☐ 5. 情報共有・ポータル ☐ 6. スケジュール共有 ☐ 7. LGWAN-ASP ☐ 8. その他（備考欄に具体的に記載）		外部サービス許可申請記録
54			外部サービスの責任分担	利用する外部サービスの情報セキュリティ対策について、外部サービスの提供者との責任の分担を定め、その実施状況を定期的に確認していますか？			外部サービス情報セキュリティ対策実施確認記録
55		緊急時対応計画等	緊急時対応計画の策定	システムの情報資産への侵害が発生した場合に備えて、あらかじめ関係機関との連絡体制や復旧対策等を定めた緊急時対応計画を策定していますか？	2.概ねしている		・緊急時対応計画
56			災害時等、緊急時の連絡体制	災害時等、緊急時の連絡体制について、連絡手順などを外部委託事業者等も含めて作成し、情報交換を円滑に行えるよう連絡体制を明確にしていますか？	1.している		・連絡体制表
57			緊急時対応計画の見直し	情報セキュリティを取り巻く状況の変化や組織体制の変動等に応じ、緊急時対応計画の規定を見直していますか？	3.どちらとも言えない		

（別添３）β/β´モデル共通の監査項目

項目			No.	監査項目	監査資料の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
1.組織体制		3)CSIRTの設置・役割	4	**Ⅲ)CSIRTの設置・役割の明確化** CSIRTが設置され、部局の情報セキュリティインシデントについてCISOへの報告がされている。また、CISOによって、CSIRT及び構成する要員の役割が明確化されている。	□情報セキュリティポリシー □CSIRT設置要綱	監査資料のレビューと統括情報セキュリティ責任者へのインタビューにより、CSIRTが設置されており、規定された役割に応じて情報セキュリティインシデントのとりまとめやCISOへの報告、報道機関等への通知、関係機関との情報共有等を行う統一的な窓口が設置されているか確かめる。また、監査資料のレビューとCISO又は構成要員へのインタビューにより、CSIRTの要員構成、役割などが明確化されており、要員はそれぞれの役割を理解しているか確かめる。	1.(9)	6.1.3 6.1.4 16.1.1 16.1.2 16.1.3 16.1.4 16.1.5	
5.人的セキュリティ	5.1.職員等の遵守事項	(1)職員等の遵守事項①情報セキュリティポリシー等の遵守	83	**Ⅰ)情報セキュリティポリシー等遵守の明記** 統括情報セキュリティ責任者又は情報セキュリティ責任者によって、職員等が情報セキュリティポリシー及び実施手順を遵守しなければならないことが定められ、文書化されている。	□情報セキュリティポリシー □職員等への周知記録	監査資料のレビューと統括情報セキュリティ責任者又は情報セキュリティ責任者へのインタビューにより、職員等の情報セキュリティポリシー及び実施手順の遵守や、情報セキュリティ対策について不明な点及び遵守が困難な点等がある場合に職員等がとるべき手順について文書化され、正式に承認されているか確かめる。また、承認された文書が職員等に周知されているか確かめる。	5.1.(1)①	5.1.1	
			84	**Ⅱ)情報セキュリティポリシー等の遵守** 職員等は、情報セキュリティポリシー及び実施手順を遵守するとともに、情報セキュリティ対策について不明な点や遵守が困難な点等がある場合、速やかに情報セキュリティ管理者に相談し、指示を仰げる体制になっている。	□情報セキュリティポリシー □実施手順書	監査資料のレビューと情報セキュリティ管理者及び職員等へのインタビューにより、情報セキュリティポリシー及び実施手順の遵守状況を確かめる。また、情報セキュリティ対策について不明な点及び遵守が困難な点等がある場合、職員等が速やかに情報セキュリティ管理者に相談し、指示を仰げる体制が整備されているか確かめる。必要に応じて、職員等へのアンケート調査を実施し、周知状況を確かめる。	5.1.(1)①	5.1.1	・職員等の情報セキュリティポリシーの遵守状況の確認及び対処については、No.314～322も関連する項目であることから参考にすること。
		(1)職員等の遵守事項②業務以外の目的での使用の禁止	86	**Ⅱ)情報資産等の業務以外の目的での使用禁止** 職員等による業務以外の目的での情報資産の持ち出し、情報システムへのアクセス、電子メールアドレスの使用及びインターネットへのアクセスは行われていない。	□端末ログ □電子メール送受信ログ □ファイアウォールログ	監査資料のレビューと情報システム管理者及び職員等へのインタビューにより、業務以外の目的での情報資産の持ち出し、情報システムへのアクセス、電子メールアドレスの使用及びインターネットへのアクセスが行われていないか確かめる。必要に応じて、職員等へのアンケート調査を実施して確かめる。	5.1.(1)②	—	
		(1)職員等の遵守事項③モバイル端末や電磁的記録媒体の持ち出し及び外部における情報処理作業の制限	88	**Ⅱ)情報資産等の外部持出制限** 職員等がモバイル端末、電磁的記録媒体、情報資産及びソフトウェアを外部に持ち出す場合、情報セキュリティ管理者により許可を得ている。	□端末等持出・持込基準/手続 □庁外での情報処理作業基準/手続 □端末等持出・持込申請書/承認書	監査資料のレビューと情報セキュリティ管理者及び職員等へのインタビューにより、職員等がモバイル端末、電磁的記録媒体、情報資産及びソフトウェアを外部に持ち出す場合、情報セキュリティ管理者から許可を得ているか確かめる。必要に応じて、職員等へのアンケート調査を実施して確かめる。	5.1.(1)③(イ)	6.2.1 6.2.2 11.2.6	・紛失、盗難による情報漏えいを防止するため、暗号化等の適切な処置をして持出すことが望ましい。
			89	**Ⅲ)外部での情報処理業務の制限** 職員等が外部で情報処理作業を行う場合は、情報セキュリティ管理者による許可を得ている。	□庁外での情報処理作業基準/手続 □庁外作業申請書/承認書	監査資料のレビューと情報セキュリティ管理者及び職員等へのインタビューにより、職員等が外部で情報処理作業を行う場合、情報セキュリティ管理者から許可を得ているか確かめる。必要に応じて、職員等へのアンケート調査を実施して確かめる。	5.1.(1)③(ウ)	6.2.1 6.2.2 11.2.6	・情報漏えい事故を防止するため、業務終了後は速やかに勤務地に情報資産を返却することが望ましい。
		(1)職員等の遵守事項④支給以外のパソコン、モバイル端末及び電磁的記録媒体の業務利用	90	**Ⅰ)支給以外のパソコン、モバイル端末及び電磁的記録媒体の業務利用基準及び手続** 統括情報セキュリティ責任者又は情報セキュリティ責任者によって、職員等が業務上支給以外のパソコン、モバイル端末及び電磁的記録媒体を利用する場合の基準及び手続について定められ、文書化されている。	□端末等持出・持込基準/手続 □支給以外のパソコン等使用申請書/承認書	監査資料のレビューと統括情報セキュリティ責任者又は情報セキュリティ責任者へのインタビューにより、支給以外のパソコン、モバイル端末及び電磁的記録媒体利用手順が文書化され、正式に承認されているか確かめる。	5.1.(1)④	8.2.3 11.2.1	
			91	**Ⅱ)支給以外のパソコン、モバイル端末及び電磁的記録媒体の利用制限** 職員等が情報処理作業を行う際に支給以外のパソコン、モバイル端末及び電磁的記録媒体を用いる場合、当該端末の業務利用の可否判断をCISOが行った後に、業務上必要な場合は、統括情報セキュリティ責任者の定める実施手順に従い、情報セキュリティ管理者による許可を得ている。また、機密性の高い情報資産の支給以外のパソコン、モバイル端末及び電磁的記録媒体による情報処理作業は行われていない。	□支給以外のパソコン等使用申請書/承認書 □支給以外のパソコン等使用基準/実施手順書	監査資料のレビューと情報セキュリティ管理者及び職員等へのインタビューにより、職員等が情報処理作業を行う際に支給以外のパソコン、モバイル端末及び電磁的記録媒体を用いる場合、情報セキュリティ管理者の許可を得ているか確かめる。また、端末のウイルスチェックが行われていること、端末ロック機能及び遠隔消去機能が利用できること、機密性3の情報資産の情報処理作業を行っていないこと、支給以外の端末のセキュリティに関する教育を受けた者のみが利用しているか確かめる。必要に応じて、職員等へのアンケート調査を実施して確かめる。また、手順書に基づいて許可や利用がされているか確かめる。	5.1.(1)④	6.2.1 6.2.2 11.2.1 11.2.6	
			92	**Ⅲ)支給以外のパソコン、モバイル端末及び電磁的記録媒体の庁内ネットワーク接続** 職員等が支給以外のパソコン、モバイル端末及び電磁的記録媒体を庁内ネットワークに接続することを許可する場合は、統括情報セキュリティ責任者又は情報セキュリティ責任者によって、情報漏えい対策が講じられている。	□庁外での情報処理作業基準/手続 □支給以外のパソコン等使用申請書/承認書 □支給以外のパソコン等使用基準/実施手順書	監査資料のレビューと情報セキュリティ管理者及び職員等へのインタビューにより、支給以外のパソコン、モバイル端末及び電磁的記録媒体を庁内ネットワークに接続することを許可する場合は、シンクライアント環境やセキュアブラウザの使用、ファイル暗号化機能を持つアプリケーションでの接続のみを許可する等の情報漏えい対策が講じられているか確かめる。必要に応じて、職員等へのアンケート調査を実施して確かめる。	5.1.(1)④	13.1.1 13.1.2	
		(1)職員等の遵守事項⑤持ち出し及び持ち込みの記録	94	**Ⅱ)端末等の持出・持込記録の作成** 情報セキュリティ管理者によって、端末等の持ち出し及び持ち込みの記録が作成され、保管されている。	□端末等持出・持込基準/手続 □端末等持出・持込申請書/承認書	監査資料のレビューと情報セキュリティ管理者へのインタビューにより、端末等の持ち出し及び持ち込みの記録が作成され、保管されているか確かめる。	5.1.(1)⑤	11.2.5	・記録を定期的に点検し、紛失、盗難が発生していないか確認することが望ましい。
		(1)職員等の遵守事項⑦机上の端末等の管理	98	**Ⅱ)机上の端末等の取扱** 離席時には、パソコン、モバイル端末、電磁的記録媒体、文書等の第三者使用又は情報セキュリティ管理者の許可なく情報が閲覧されることを防止するための適切な措置が講じられている。	□クリアデスク・クリアスクリーン基準	監査資料のレビューと情報セキュリティ管理者及び職員等へのインタビュー、執務室の視察により、パソコン、モバイル端末の画面ロックや電磁的記録媒体、文書等の容易に閲覧されない場所への保管といった、情報資産の第三者使用又は情報セキュリティ管理者の許可なく情報が閲覧されることを防止するための適切な措置が講じられているか確かめる。必要に応じて、職員等へのアンケート調査を実施して確かめる。	5.1.(1)⑦	11.2.9	
		(3)情報セキュリティポリシー等の掲示	106	**Ⅱ)情報セキュリティポリシー等の掲示** 情報セキュリティ管理者によって、職員等が常に最新の情報セキュリティポリシー及び実施手順を閲覧できるように掲示されている。	□職員等への周知記録	監査資料のレビューと情報セキュリティ管理者へのインタビュー及び執務室の視察により、職員等が常に最新の情報セキュリティポリシー及び実施手順を閲覧できるよう、イントラネット等に掲示されているか確かめる。	5.1.(3)	5.1.1	
		(4)外部委託事業者に対する情報セキュリティポリシー等遵守の説明	108	**Ⅱ)委託事業者に対する情報セキュリティポリシー等遵守の説明** ネットワーク及び情報システムの開発・保守等を委託事業者に発注する場合、情報セキュリティ管理者によって、情報セキュリティポリシー等のうち、委託事業者及び再委託事業者が守るべき内容の遵守及びその機密事項が説明されている。	□業務委託契約書 □委託管理基準	監査資料のレビューと情報セキュリティ管理者へのインタビューにより、ネットワーク及び情報システムの開発・保守等を発注する委託事業者及び再委託事業者に対して、情報セキュリティポリシー等のうち委託事業者等が守るべき内容の遵守及びその機密事項が説明されているか確かめる。	5.1.(4)	15.1.1 15.1.2	・再委託は原則禁止であるが、例外的に再委託を認める場合には、再委託事業者における情報セキュリティ対策が十分取られており、委託事業者と同等の水準であることを確認した上で許可しなければならない。・委託事業者に対して、契約の遵守等について必要に応じ立ち入り検査を実施すること。・委託に関する事項については、No.337～366も関連する項目であることから参考にすること。
	5.2.研修・訓練	(1)情報セキュリティに関する研修・訓練	110	**Ⅱ)情報セキュリティ研修・訓練の実施** CISOによって、定期的にセキュリティに関する研修・訓練が実施されている。	□研修・訓練実施基準 □研修実施報告書 □訓練実施報告書	監査資料のレビューと統括情報セキュリティ責任者へのインタビューにより、定期的に情報セキュリティに関する研修・訓練が実施されているか確かめる。	5.2.(1)	7.2.2	
	5.3.情報セキュリティインシデントの報告		121	**Ⅰ)情報セキュリティインシデントの報告手順** 統括情報セキュリティ責任者によって、情報セキュリティインシデントを認知した場合の報告手順が定められ、文書化されている。	□情報セキュリティインシデント報告手順書	監査資料のレビューと統括情報セキュリティ責任者又は情報セキュリティ責任者へのインタビューにより、職員等が情報セキュリティインシデントを認知した場合、又は住民等外部から情報セキュリティインシデントの報告を受けた場合の報告ルート及びその方法が文書化され、正式に承認されているか確かめる。	5.3.(1)～(3)	16.1.2 16.1.3	・報告ルートは、団体の意思決定ルートと整合していることが重要である。
		(1)庁内での情報セキュリティインシデントの報告	122	**Ⅰ)庁内での情報セキュリティインシデントの報告** 庁内で情報セキュリティインシデントが認知された場合、報告手順に従って関係者に報告されている。	□情報セキュリティインシデント報告手順書 □情報セキュリティインシデント報告書	監査資料のレビューと統括情報セキュリティ責任者又は情報セキュリティ責任者、情報セキュリティ管理者、情報システム管理者、職員等へのインタビューにより、報告手順に従って遅滞なく報告されているか確かめる。	5.3.(1)	16.1.2 16.1.3	
	5.4.ID及びパスワード等の管理	(1)ICカード等の取扱い	128	**Ⅲ)盗証用ICカード等の放置禁止** 認証用ICカード等を業務上必要としないときは、カードリーダーやパソコン等の端末のスロット等から抜かれている。	□ICカード等取扱基準	監査資料のレビューと情報システム管理者及び職員等へのインタビュー並びに執務室の視察により、業務上不要な場合にカードリーダーやパソコン等の端末のスロット等から認証用のICカードやUSBトークンが抜かれているか確かめる。必要に応じて、職員等へのアンケート調査を実施して確かめる。	5.4.(1)①(イ)	9.2.1 9.2.2	
			129	**Ⅳ)盗証用ICカード等の紛失時手続** 認証用ICカード等が紛失した場合は、速やかに統括情報セキュリティ責任者及び情報システム管理者に通報され、指示に従わせている。	□ICカード等取扱基準 □ICカード紛失届書	監査資料のレビューと統括情報セキュリティ責任者及び情報システム管理者へのインタビューにより、認証用のICカードやUSBトークンが紛失した場合は、速やかに統括情報セキュリティ責任者及び情報システム管理者に通報され、指示に従わせているか確かめる。	5.4.(1)①(ウ)	9.2.1 9.2.2	
			130	**Ⅴ)盗証用ICカード等の紛失時対応** 認証用ICカード等の紛失連絡があった場合、統括情報セキュリティ責任者及び情報システム管理者によって、当該ICカード等の不正使用を防止する対応がとられている。	□ICカード等取扱基準 □ICカード等管理台帳	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、紛失した認証用のICカードやUSBトークンを使用したアクセス等が速やかに停止されているか確かめる。	5.4.(1)②	9.2.1 9.2.2	
			131	**Ⅵ)盗証用ICカード等の回収及び廃棄** ICカード等を切り替える場合、統括情報セキュリティ責任者及び情報システム管理者によって、切替え前のカードが回収され、不正使用されないような措置が講じられている。	□ICカード等取扱基準 □ICカード等管理台帳	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、認証用のICカードやUSBトークンを切り替える場合に切替え前のICカードやUSBトークンが回収され、破砕するなど復元不可能な処理を行った上で廃棄されているか確かめる。	5.4.(1)③	9.2.1 9.2.2	・回収時の個数を確認し、紛失・盗難が発生していないか確実に確認することが望ましい。
	5.4.ID及びパスワード等の管理	(3)パスワードの取扱い	136	**Ⅱ)パスワードの取扱い** 職員等のパスワードは当該本人以外に知られないように取扱われている。	□パスワード管理基準	監査資料のレビューと情報システム管理者及び職員等へのインタビューにより、職員等のパスワードについて照会に応じたり、容易に想像できるような文字列に設定したりしないように取り扱われているか確かめる。必要に応じて、職員等へのアンケート調査を実施して確かめる。	5.4.(3)①～③	9.3.1	内閣サイバーセキュリティセンター(NISC)のハンドブックでは、「ログイン用パスワード」は、英大文字(26種類)小文字(26種類)＋数字(10種類)＋記号(26種類)の計88種類の文字をランダムに使って、10桁以上を安全圏として推奨している。
			137	**Ⅲ)パスワードの不正使用防止** パスワードが流出したおそれがある場合、不正使用されない措置が講じられている。	□パスワード管理基準	監査資料のレビューと情報システム管理者及び職員等へのインタビューにより、パスワードが流出したおそれがある場合、速やかに情報セキュリティ管理者に報告され、パスワードが変更されているか確かめる。必要に応じて、職員等へのアンケート調査を実施して確かめる。	5.4.(3)④	9.3.1	
			140	**Ⅵ)パスワード記憶機能の利用禁止** サーバ、ネットワーク機器及びパソコン等の端末にパスワードが記憶されていない。	□パスワード管理基準	監査資料のレビューと情報システム管理者及び職員等へのインタビュー、執務室の視察により、サーバ、ネットワーク機器及びパソコン等の端末にパスワードが記憶されていないか確かめる。必要に応じて、職員等へのアンケート調査を実施して確かめる。	5.4.(3)⑦	9.3.1	

（別添３）β´モデルを採用する場合の追加監査項目

項目		No.	監査項目	監査資料の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
3.情報システム全体の強靭性の向上	技術的対策	1	**ⅰ）無害化処理** CISO又は統括情報セキュリティ責任者によって、LGWAN接続系にインターネット接続系からファイルを取り込む際に、以下の対策が実施されている。 ・ファイルからテキストのみを抽出 ・ファイルを画像PDFに変換 ・サニタイズ処理 ・インターネット接続系において内容を目視で確認するとともに、未知の不正プログラム検知及びその実行を防止する機能を有するソフトウェアで危険因子の有無を確認	□システム構成図 □システム設計書 □機器等の設定指示書 □運用手順書	監査資料のレビューとCISO又は統括情報セキュリティ責任者へのインタビューにより、LGWAN接続系にインターネット接続系からファイルを取り込む際に、ファイルからテキストのみを抽出、ファイルを画像PDFに変換、サニタイズ処理、インターネット接続系において内容を目視で確認するとともに、未知の不正プログラム検知及びその実行を防止する機能を有するソフトウェアで危険因子の有無を確認するなどの対策が実施されているか確かめる。	3.(3)	―	・無害化の処理方法が複数ある場合は、それぞれの方法について実施状況を確認する。
		2	**ⅱ）LGWAN接続系の画面転送** CISO又は統括情報セキュリティ責任者によって、以下の対応が全て実施されている。 ・インターネット接続系の業務端末からLGWAN接続系のサーバや端末を利用する場合は、仮想化されたリモートデスクトップ形式で接続されている。 ・LGWAN接続系からインターネット接続系へのデータ転送(クリップボートのコピー&ペースト等)が禁止されている。ただし、LGWANメールやLGWANからの取り込み、業務で必要となるデータの転送については、中継サーバやファイアウォール等を設置し、通信ポート、IPアドレス、MACアドレス等で通信先を限定することで可能とされている。	□システム構成図 □システム設計書 □機器等の設定指示書 □運用手順書	監査資料のレビューとCISO又は統括情報セキュリティ責任者へのインタビューにより、インターネット接続系の業務端末からLGWAN接続系のサーバや端末を利用する場合は、仮想化されたリモートデスクトップ形式で接続されていることを確認する。さらに、LGWAN接続系からインターネット接続系へのデータ転送(クリップボートのコピー&ペースト等)が原則禁止されており、通信先を限定されたLGWANメールやLGWANからの取り込み、業務で必要となるデータの転送のみが許可されていることを確かめる。	3.(3)	―	
		3	**ⅲ）未知の不正プログラム対策（エンドポイント対策）** 統括情報セキュリティ責任者及び情報システム管理者により、パターンマッチング型の検知に加えて、セキュリティ専門家やSOC等のマネージドサービスの運用によって、以下の対応が全て実施されている。 ・端末等のエンドポイントにおけるソフトウェア等の動作を監視し、未知及び既知のマルウェア等による悪意ある活動を示す異常な挙動を監視・検出・特定する。 ・異常な挙動を検出した際にプロセスを停止、ネットワークからの論理的な隔離を行う。 ・インシデント発生時に発生要因の詳細な調査を実施する。	□システム構成図 □システム設計書 □機器等の設定指示書 □運用手順書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、パターンマッチング型の検知に加えて、セキュリティ専門家やSOC等のマネージドサービスの運用によって、端末等のエンドポイントにおけるソフトウェア等の動作の監視がされていること、未知及び既知のマルウェア等の異常な挙動を監視・検知・特定ができるようになっていること並びに異常な挙動を検出した際のプロセスの停止、異常な挙動が検知された端末等に対してネットワークからの隔離ができるようになっていること及びインシデント発生要因の詳細な調査が実施できるようになっていることを確かめる。	3.(3)	―	
		4	**ⅳ）業務システムログ管理** 統括情報セキュリティ責任者及び情報システム管理者によって、インターネット接続系の業務システムのログの収集、分析、保管が実施されている。	□システム運用基準 □ログ □システム稼動記録 □障害時のシステム出力ログ	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、インターネット接続系の業務システムに関するログが適切に収集、分析、保管されていることを確かめる。	3.(3)	・ログの取得及び保管についてはNo.156～159も関連する項目であることから参考にすること。	
		5	**ⅴ）情報資産単位でのアクセス制御** 統括情報セキュリティ責任者又は情報システム管理者によって、アクセス制御に関わる方針及び基準が定められ、文書化されており、基準に従ってアクセス制御されている。文書を管理するサーバ等は課室単位でのアクセス制御を実施している。	□アクセス制御方針 □アクセス管理基準 □システム設計書 □機器等の設定指示書	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、情報資産の機密性レベルに応じて業務システム単位でのアクセス制御が行われていること、文書を管理するサーバ等で課室単位でのアクセス制御が実施されていることを確かめる。	3.(3)	・アクセス制御についてはNo.216～241も関連する項目であることから参考にすること。	
		6	**ⅵ）脆弱性管理** 統括情報セキュリティ責任者及び情報システム管理者によって、OSやソフトウェアのバージョンなどが漏れなく資産管理され、脆弱性の所在が効率的に把握されており、深刻度に応じて修正プログラムを適用し、ゼロデイ攻撃等のソフトウェアの脆弱性を狙った攻撃に迅速に対応されている。	□情報セキュリティ関連情報の通知記録 □脆弱性関連情報の通知記録 □サイバー攻撃情報やインシデント情報の通知記録 □脆弱性対応計画	監査資料のレビューと統括情報セキュリティ責任者又は情報システム管理者へのインタビューにより、OSやソフトウェアのバージョンなどが漏れなく資産管理され、脆弱性の所在が効率的に把握されており、深刻度に応じて修正プログラムを適用し、ゼロデイ攻撃等のソフトウェアの脆弱性を狙った攻撃に迅速に対応できるようになっているか確かめる。	3.(3)	・脆弱性管理についてはNo.304～308も関連する項目であることから参考にすること。	
	組織的・人的対策	7	**ⅰ）セキュリティの継続的な検知・モニタリング体制の整備** 職員等の標的型攻撃訓練や研修等の受講状況や結果を確認し、セキュリティ対策の浸透状況や効果が測定されており、その結果がフィードバックされている。	□研修・訓練実施基準 □研修・訓練実施計画 □研修・訓練受講記録 □研修・訓練結果報告書 □研修・訓練に関するアンケート	監査資料のレビューと統括情報セキュリティ責任者へのインタビューにより、標的型攻撃訓練や研修等の受講状況や結果を確認し、セキュリティ対策の浸透状況や効果が測定されており、その結果がフィードバックされているか確かめる。	3.(3)	・標的型訓練についても計画に含めることが望ましい。	
		8	**ⅰ）住民に関する情報をインターネット接続系に保存させない規定の整備** 住民に関する情報資産は特に重要な情報資産であるため、インターネット接続系のファイルサーバに保存させないことや、一時的に保存したとしても直ちに削除すること等が規定として定められており、その規定に従い、運用がされている。	□情報資産管理基準 □実施手順書	監査資料のレビューと統括情報セキュリティ責任者へのインタビューにより、住民情報に関する情報の取扱いについて文書化され、運用されており、実際に住民情報に関する情報がインターネット接続系のファイルサーバ等に保存されていないことを確かめる。	3.(3)	―	
		9	**ⅲ）情報セキュリティ研修、標的型攻撃訓練、セキュリティインシデント訓練の受講** 職員等が情報セキュリティ研修、標的型攻撃訓練を年1回以上受講しており、情報システム管理者、情報システム担当者がセキュリティインシデントが発生した場合の訓練を年1回以上受講している。	□研修・訓練実施基準 □研修・訓練実施計画 □研修・訓練受講記録 □研修・訓練結果報告書 □研修・訓練に関するアンケート	監査資料のレビューと統括情報セキュリティ責任者及び職員等へのインタビューにより、職員等が情報セキュリティ研修、標的型攻撃訓練を年1回以上受講していること及び情報システム管理者、情報システム担当者がセキュリティインシデントが発生した場合の訓練を年1回以上受講していることを確かめる。	3.(3)	―	
		10	**ⅳ）情報セキュリティ研修計画** 職員等が毎年度最低1回は情報セキュリティ研修を受講できるように計画されている。	□研修・訓練実施基準 □研修・訓練実施計画	監査資料のレビュー又は統括情報セキュリティ責任者へのインタビューにより、研修計画において、職員等が毎年度最低1回は情報セキュリティ研修を受講できるように計画されているか確かめる。	3.(3)	7.2.2	・αモデルにおいては推奨事項だが、β・β´モデルにおいては必須事項となる。
		11	**Ⅴ）実践的サイバー防御演習（CYDER）の確実な受講** CISOによって、実践的サイバー防御演習（CYDER）を受講しなければならないことが定められ、受講計画が策定されており、また、受講計画に従い、職員等が受講している。	□研修・訓練実施計画 □研修・訓練受講記録 □研修・訓練結果報告書	監査資料のレビュー又は統括情報セキュリティ責任者へのインタビューにより、実践的サイバー防御演習（CYDER）の受講計画について文書化され、正式に承認されているか確かめる。また、職員等が適切に受講しており、その受講記録が取られていることを確かめる。	3.(3)	―	
		12	**Ⅵ）演習等を通じたサイバー攻撃情報やインシデント等への対策情報共有** 職員等が以下の演習やそれに準ずる演習を受講している。 ・インシデント対応訓練（基礎/高度） ・分野横断的演習	□研修・訓練実施計画 □研修・訓練受講記録 □研修・訓練結果報告書	監査資料のレビュー又は統括情報セキュリティ責任者へのインタビューにより、職員等がインシデント対応訓練（基礎/高度）、分野横断的演習又はそれに準ずる演習を受講しているか確かめる。	3.(3)	―	
		13	**Ⅶ）自治体情報セキュリティポリシーガイドライン等の見直しを踏まえた情報セキュリティポリシーの見直し** 自治体情報セキュリティポリシーガイドライン等の見直し踏まえて、適時適切に情報セキュリティポリシーの見直しがされている。	□情報セキュリティポリシー	監査資料のレビュー又は統括情報セキュリティ責任者へのインタビューにより、情報セキュリティポリシーが自治体情報セキュリティポリシーガイドライン等の見直しを踏まえて、適時適切に見直しがされていることを確かめる。	―	―	・情報セキュリティポリシーの策定・遵守については、No.314-322、No.367-377、No.384-385も関連する項目であることから参考にすること。